

DECYZJA JEDNOLITEJ RADY DS. RESTRUKTURYZACJI I UPORZĄDKOWANEJ LIKWIDACJI**z dnia 18 września 2019 r.****w sprawie wewnętrznych zasad dotyczących ograniczenia pewnych praw osób, których dane dotyczą, w związku z przetwarzaniem danych osobowych w ramach dochodzeń wewnętrznych w sprawie zdarzenia naruszającego ochronę prowadzonych przez Jednolitą Radę ds. Restrukturyzacji i Uporządkowanej Likwidacji (SRB/ES/2019/34)**

JEDNOLITA RADA DS. RESTRUKTURYZACJI I UPORZĄDKOWANEJ LIKWIDACJI,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 806/2014 z dnia 15 lipca 2014 r. ustanawiające jednolite zasady i jednolitą procedurę restrukturyzacji i uporządkowanej likwidacji instytucji kredytowych i niektórych firm inwestycyjnych w ramach jednolitego mechanizmu restrukturyzacji i uporządkowanej likwidacji oraz jednolitego funduszu restrukturyzacji i uporządkowanej likwidacji oraz zmieniające rozporządzenie (UE) nr 1093/2010⁽¹⁾, w szczególności jego art. 42, art. 43 ust. 5, art. 50 ust. 3, art. 56 ust. 1–3, art. 61, 63 i 64,uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE⁽²⁾,

uwzględniając konsultacje z Europejskim Inspektorem Ochrony Danych,

a także mając na uwadze, co następuje:

- (1) Jednolita Rada ds. Restrukturyzacji i Uporządkowanej Likwidacji (Single Resolution Board – „**SRB**”) pełni rolę organu ds. restrukturyzacji i uporządkowanej likwidacji w ramach jednolitego mechanizmu restrukturyzacji i uporządkowanej likwidacji (Single Resolution Mechanism – „**SRM**”) zgodnie z rozporządzeniem (UE) nr 806/2014. Misją SRB jest zapewnienie, aby restrukturyzacja i uporządkowana likwidacja banków znajdujących się w trudnej sytuacji przebiegały w sposób uporządkowany, wywierając jak najmniejszy wpływ na gospodarkę realną, system finansowy i finanse publiczne uczestniczących państw członkowskich i innych państw.
- (2) SRB może przetwarzać dane osobowe w ramach różnych systemów funkcjonujących na terenie SRB (monitoring wizyjny, kontrola dostępu, rejestry odwiedzających). Informacje te są gromadzone ściśle ze względów bezpieczeństwa (np. w celu śledzenia liczby osób w budynku na potrzeby potencjalnej ewakuacji, co jest zgodne z decyzjami Komisji Europejskiej w zakresie bezpieczeństwa) w celu zapobiegania zdarzeniom naruszającym ochronę w budynkach lub ich otoczeniu, wykrywania takich zdarzeń i ich dokumentowania.
- (3) SRB, reprezentowana w tym przypadku przez kierownika swojego Działu Obsługi Administracyjnej i ICT, przetwarza kilka kategorii danych osobowych, w szczególności dane umożliwiające identyfikację, dane kontaktowe i dane służbowe. Dane osobowe są przechowywane w zabezpieczonym środowisku elektronicznym uniemożliwiającym bezprawny dostęp lub przekazanie danych osobom, które nie muszą mieć do nich dostępu. Przetwarzane dane osobowe są zatrzymywane zgodnie z zasadami KE dotyczącymi zatrzymywania danych. Po upływie okresu zatrzymania zgromadzone informacje, w tym dane osobowe, są usuwane stosownie do uzgodnionego okresu maksymalnego zatrzymania danych: rejestry odwiedzających: 6 miesięcy, nagrania z monitoringu wizyjnego: 30 dni, system kontroli dostępu: 2 miesiące.
- (4) Wewnętrzne zasady powinny mieć zastosowanie do wszystkich procesów przetwarzania prowadzonych przez SRB w ramach realizacji jej działalności dla celów bezpieczeństwa, zapobiegania zdarzeniom naruszającym ochronę, wykrywania ich lub prowadzenia dochodzeń w ich sprawie, ochrony personelu, własności i informacji agencji, a także odwiedzających SRB.
- (5) Wewnętrzne zasady powinny mieć zastosowanie do procesów przetwarzania prowadzonych w trakcie wewnętrznych dochodzeń w sprawie zdarzeń naruszających ochronę, a także w trakcie monitorowania działań następczych podejmowanych w rezultacie tych dochodzeń. Wewnętrzne zasady powinny mieć zastosowanie do procesów przetwarzania, które stanowią część działań powiązanych z sekcją bezpieczeństwa/infrastruktury SRB. Powinny one również obejmować pomoc i współpracę ze strony sekcji bezpieczeństwa/infrastruktury SRB udzielaną organom krajowym, belgijskim organom ścigania, OLAF, służbom ratunkowym i organizacjom międzynarodowym poza dochodzeniami administracyjnymi.
- (6) SRB musi przedstawić uzasadnienie ścisłej konieczności i proporcjonalności ograniczeń w społeczeństwie demokratycznym oraz postępować z poszanowaniem istoty podstawowych praw i wolności;

⁽¹⁾ Dz.U. L 225 z 30.7.2014, s. 1.⁽²⁾ Dz.U. L 295 z 21.11.2018, s. 39.

- (7) W ramach powyższego SRB ma obowiązek przestrzegać w możliwie szerokim zakresie w trakcie realizacji powyższych procedur praw podstawowych osób, których dane dotyczą, w szczególności tych związanych z prawem dostępu, prawem do sprostowania danych, prawem do usunięcia danych, prawem do przenoszenia danych itp., które to przewidziano w rozporządzeniu (UE) 2018/1725.
- (8) Tym niemniej SRB może być zobowiązana do wstrzymania przekazania informacji osobie, której dane dotyczą, lub wykonania innych praw osoby, której dane dotyczą, w celu zabezpieczenia – w szczególności – własnych dochodzeń w sprawie zdarzeń naruszających ochronę, w tym danych z monitoringu wizyjnego lub systemów kontroli dostępu.
- (9) SRB może zatem wstrzymać przekazanie informacji w celu zabezpieczenia dochodzeń w sprawie zdarzeń naruszających ochronę.
- (10) SRB powinna znieść ograniczenia, gdy tylko przestaną występować warunki uzasadniające ograniczenie.
- (11) SRB powinna regularnie, w odstępach sześciu miesięcy, monitorować warunki ograniczające i w razie konieczności dokonywać ich rewizji.
- (12) SRB powinna w trakcie dokonywania rewizji konsultować się z inspektorem ochrony danych,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Przedmiot i zakres stosowania

1. Niniejsza decyzja określa wewnętrzne zasady dotyczące warunków, w których SRB w ramach wewnętrznych dochodzeń w sprawie zdarzenia naruszającego ochronę może zgodnie z art. 25 rozporządzenia (UE) 2018/1725 ograniczyć stosowanie praw przewidzianych w art. 14–21 i 35, jak również art. 4.
2. Decyzja ma zastosowanie do procesu (procesów) przetwarzania przez SRB danych osobowych na potrzeby prowadzenia wewnętrznych dochodzeń w sprawie zdarzenia naruszającego ochronę, a także podczas monitorowania działań następczych podejmowanych w rezultacie takich dochodzeń.
3. Do kategorii danych podlegających przetwarzaniu należą tzw. dane twarde (dane administracyjne, numer telefonu, prywatny adres, środki łączności elektronicznej i dane o ruchu) lub tzw. dane miękkie (oceny, wszczęcia postępowań wyjaśniających, sprawozdania z dochodzeń wstępnych) itp.
4. Z zastrzeżeniem warunków określonych w niniejszej decyzji ograniczenia te mogą mieć zastosowanie do następujących praw: prawo dostępu do informacji, prawo do sprostowania, prawo do usunięcia i prawo do przenoszenia, prawo do informacji, poufność komunikacji, jak również do zasad procesu przetwarzania danych, o ile mają one związek z którymkolwiek z praw.

Artykuł 2

Wyznaczenie administratora i zabezpieczenia

1. W celu uniknięcia naruszenia, wycieku lub nieuprawnionego ujawnienia danych wprowadzono następujące zabezpieczenia: ograniczenie praw dostępu do folderów elektronicznych oraz funkcyjnej skrzynki pocztowej służącej do składania skarg, szafka na klucz, szczegółowe szkolenie dotyczące poufności dla osób przetwarzających informacje.
2. Administratorem tych procesów przetwarzania jest SRB, reprezentowana w tym przypadku przez kierownika Działu Obsługi Administracyjnej i ICT SRB.
3. Dane osobowe są zbierane i zatrzymywane zgodnie z zasadami KE dotyczącymi zatrzymywania danych oraz zgodnie z belgijską ustawą z dnia 21 marca 2007 r. (regulującą montaż i wykorzystanie kamer monitoringu). Dane są zatrzymywane zgodnie z zasadą, w myśl której danych nie zatrzymuje się na okres dłuższy niż jest to konieczne do realizacji procesu przetwarzania i – ewentualnie – rozstrzygnięcia sporów sądowych lub administracyjnych.

Artykuł 3

Ograniczenia

1. Zgodnie z art. 25 ust. 1 rozporządzenia (UE) 2018/1725 wszelkie ograniczenia mają zastosowanie jedynie w celu:
 - zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom,
 - zabezpieczenia bezpieczeństwa wewnętrznego instytucji i organów Unii, w tym ich sieci łączności elektronicznej,
 - ochrony postępowania sądowego,
 - zapobiegania naruszeniom zasad etyki w zawodach regulowanych, prowadzenia postępowań w takich sprawach, ich wykrywania oraz ścigania,
 - ochrony osoby, której dane dotyczą, lub praw i wolności innych osób.
2. Ograniczenia muszą być ściśle konieczne i proporcjonalne w społeczeństwie demokratycznym oraz zgodne z poszanowaniem istoty podstawowych praw i wolności.
3. Test konieczności i proporcjonalności należy przeprowadzić w oparciu o obowiązujące zasady wewnętrzne. Proces ten zostaje udokumentowany wewnętrzną notą oceny dla celów rozliczalności, osobno dla każdego przypadku.
4. Ograniczenia są należycie monitorowane i poddawane okresowej weryfikacji co sześć miesięcy.
5. Ograniczenia są znoszone, gdy tylko przestają występować okoliczności uzasadniające ich stosowanie.
6. Ryzykiem dla praw i wolności osób, których dane dotyczą, jest czasowe ograniczenie skutecznego wykonywania praw osób, których dane dotyczą, między innymi prawa do informacji, prawa do usunięcia danych czy prawa do obrony, przewidzianych w rozporządzeniu (UE) 2018/1725. Ryzyko to powinno być uwzględnione w zakresie testu konieczności i proporcjonalności, o którym mowa w ust. 3 niniejszego artykułu.

Artykuł 4

Zaangażowanie inspektora ochrony danych

1. SRB w trakcie procedury ograniczania praw informuje inspektora ochrony danych SRB („inspektora ochrony danych”) bez zbędnej zwłoki o wprowadzonych ograniczeniach zastosowania praw osób, których dane dotyczą, zgodnie z niniejszą decyzją. SRB udziela dostępu do dokumentacji oraz oceny konieczności i proporcjonalności tego ograniczenia.
2. Inspektor ochrony danych może na piśmie wymagać od administratora przedstawienia przeglądu stosowania ograniczeń. SRB informuje inspektora ochrony danych na piśmie o rezultatach żadanego przeglądu i zniesieniu ograniczenia, gdy to nastąpi.

Artykuł 5

Udzielanie informacji osobom, których dane dotyczą

1. SRB uwzględnia w klauzuli o ochronie danych opublikowanej w intranecie i na stronie internetowej, zawierającej informację o prawach przysługujących w ramach danej procedury osobom, których dane dotyczą, informacje dotyczące ewentualnego ograniczenia tych praw. Informacja zawiera wskazanie danych, które mogą podlegać ograniczeniu, przyczyny ograniczenia oraz potencjalny okres obowiązywania ograniczenia.
2. Ponadto SRB, bez uszczerbku dla kolejnego ustępu, bez zbędnej zwłoki i w formie pisemnej informuje indywidualnie osoby, których dane dotyczą, o ich prawach dotyczących obecnych lub przyszłych ograniczeń.
3. Osoby, których dane dotyczą, są informowane o głównych przyczynach zastosowania ograniczenia oraz prawie do wniesienia skargi do Europejskiego Inspektora Ochrony Danych.

Artykuł 6

Prawo dostępu do danych przez osobę, której dane dotyczą

1. Jeżeli osoby, których dane dotyczą, żądają dostępu do swoich danych osobowych przetwarzanych w kontekście co najmniej jednej sprawy lub konkretnej operacji przetwarzania, zgodnie z art. 17 rozporządzenia (UE) 2018/1725 SRB ogranicza się w ocenie wniosku wyłącznie do takich danych osobowych.
2. Jeżeli SRB ogranicza, w całości lub częściowo, prawo dostępu, o którym mowa w art. 17 rozporządzenia (UE) 2018/1725, podejmuje następujące kroki:
 - a) w odpowiedzi na wniosek informuje osobę, której dane dotyczą, o stosowanym ograniczeniu i jego głównych przyczynach, jak również o możliwości złożenia skargi do Europejskiego Inspektora Ochrony Danych i możliwości skorzystania ze środka ochrony prawnej przed Trybunałem Sprawiedliwości Unii Europejskiej;
 - b) dokumentuje przyczyny ograniczenia, w tym ocenę jego konieczności i proporcjonalności; w tym celu dokumentacja określa, w jaki sposób udzielenie dostępu do danych zagroziłoby działalności dochodzeniowej SRB lub ograniczeniom stosowanym na podstawie art. 2 ust. 3. bądź też negatywnie wpłynęłoby na prawa i wolności innych osób, których dane dotyczą.

Zgodnie z art. 25 ust. 8 rozporządzenia (UE) 2018/1725 można wstrzymać przekazanie informacji, o których mowa w lit. a), pominąć je lub odmówić go.

3. Dokumentacja, o której mowa w ust. 2 lit. b), jak również – w stosownych przypadkach – dokumenty zawierające informację o okolicznościach faktycznych i prawnych stanowiących jej podstawę – są rejestrowane. Udostępnia się je Europejskiemu Inspektorowi Ochrony Danych na żądanie. Zastosowanie ma art. 25 ust. 7 rozporządzenia (UE) 2018/1725.

Artykuł 7

Prawo do sprostowania, usunięcia i ograniczenia przetwarzania

Jeżeli SRB ogranicza w całości lub częściowo stosowanie prawa do sprostowania danych, ich usunięcia lub ograniczenia przetwarzania, o których mowa w art. 18, art. 19 ust. 1 i art. 20 ust. 1 rozporządzenia (UE) 2018/1725, podejmuje kroki określone w art. 6 ust. 2 niniejszej decyzji oraz dokonuje wpisu w rejestrze zgodnie z art. 6 ust. 3 decyzji.

Artykuł 8

Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

Jeżeli SRB ogranicza prawo do zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, o którym mowa w art. 35 rozporządzenia (UE) 2018/1725, dokumentuje i rejestruje powody ograniczenia zgodnie z art. 3 ust. 3 niniejszej decyzji. Zastosowanie ma art. 3 ust. 4 niniejszej decyzji.

Artykuł 9

Wejście w życie

Niniejsza decyzja wchodzi w życie następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej.

Sporządzono w Brukseli dnia 18 września 2019 r.

W imieniu Jednolitej Rady ds. Restrukturyzacji i
Uporządkowanej Likwidacji
Elke KÖNIG
Przewodniczący